Hewlett Packard Enterprise

HPE Aruba Networking Central On-Premises 3.0.4.2

Release Notes

Copyright

Copyright Information

© Copyright 2026 Hewlett Packard Enterprise Development LP.

Open Source Code

This product includes code licensed under certain open source licenses which require source compliance. The corresponding source for these components is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, please check if the code is available in the HPE Software Center at https://myenterpriselicense.hpe.com/cwp-ui/software but, if not, send a written request for specific software version and product for which you want the open source code. Along with the request, please send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company

Attn: General Counsel

WW Corporate Headquarters

1701 E Mossy Oaks Rd, Spring, TX 77389

United States of America

Legal disclaimer

The resource assets in this document may include abbreviated and/or legacy terminology for products. See **www.arubanetworks.com** for current and complete product lines and names.

Contents

About this Guide 4
- Related Documents 4
- Conventions 4
- Contacting Support 5

3.0.4.2 What's New 6

3.0.4.2 Resolved Issues 7

3.0.4.2 Known Issues 8

API Change Log in 3.0.4.x Release 15

About this Guide

This release notes describes the new features supported by HPE Aruba Networking Central On-Premises for the release and lists the known and resolved issues.

Related Documents

- HPE Aruba Networking Central On-Premises Installation and Setup Guide
- HPE Aruba Networking Central On-Premises Non-Appliance Installation and Setup Guide
- HPE Aruba Networking Central On-Premises User Guide
- HPE GreenLake Account Home User Guide

Conventions

The following conventions are used throughout this guide to emphasize important concepts:

Table 1: Typographical Conventions

Type Style	Description
Italics	This style is used to emphasize important terms and to mark the titles of books.
`System items`	This fixed - width font depicts the following: • Sample screen output • System prompts

NOTE: Indicates helpful suggestions, pertinent information, and important things to remember.

CAUTION: Indicates a risk of damage to your hardware or loss of data.

WARNING: Indicates a risk of personal injury or death.

Contacting Support

Table 2: Contact Information

Main Site	**arubanetworking.hpe.com**
Support Site	**networkingsupport.hpe.com**
Airheads Social Forums and Knowledge Base	**community.arubanetworks.com**
North American Telephone	1 - 800 - 943 - 4526 (Toll Free)
International Telephone	**arubanetworks.com/support - services/contact - support/**
Software Licensing Site	**licensemanagement.hpe.com**
End - of - life Information	**networkingsupport.hpe.com/end - of - life**
Security Incident Response Team	Site: **arubanetworks.com/support - services/security - bulletins/** Email: **aruba - sirt@hpe.com**

3.0.4.2 What's New

This release does not include any new features or enhancements.

Attention

When version **3.0.4.0** becomes available for download, all deployments must be upgraded to **3.0.4.0** before September 30, 2026 to ensure uninterrupted service. All applications and services will be automatically shut down on **September 30, 2026, at 12:00 AM UTC**. Beginning October 31, 2026, deployments running earlier versions will no longer be supported. As part of this transition, core platform components are updated in version 3.0.4.0.

Failure to complete the upgrade by the specified date will result in the automatic shutdown of all applications and services, and the WebUI will become inaccessible. Devices will not be served and network connectivity will be impacted. If you have not upgraded by September 30, 2026, contact the TAC team to upgrade before October 31, 2026.

Starting **October 31, 2026**, users will have to perform a fresh installation of the setup.

Starting **August 01, 2026**, an **Action Required** pop-up notification will appear upon login, reminding to complete the upgrade. This reminder will be displayed once per session. In addition, alerts and audit trails will be sent weekly until one week prior to the shutdown date. During the final week, alerts and audit trails will be sent daily.

Figure 1: Action Required Pop-up Window for Users with Read-only Access

Users with read-only access should contact the network administrator to upgrade their deployments.

Figure 2: Action Required Pop-up Window for Users with Upgrade Access

Users with upgrade access can upgrade their deployments by clicking **Go to Version** in the **Action Required** pop-up notification.

3.0.4.2 Resolved Issues

The following sections provide a comprehensive list of resolved issues for the 3.0.4.2 release:

Table 3: System Management Resolved Issues

Issue ID	Description
CNX-283388	A new installation of HPE Aruba Networking Central On-Premises 3.0.4.0 with IPv6 ULA (Unique Local Address) failed during the system-ivt-stage. This issue occurred because the SSH daemon (SSHD) did not recognize the source IPv6 pod address during the installation process. The fix ensures that HPE Aruba Networking Central On-Premises 3.0.4.0 installation completes successfully with a ULA IPv6 address.
CNX-283777	Cluster onboarding intermittently failed because a service update at the end of the process conflicted with an existing service that had not been fully removed. The issue is fixed the by increasing the retry window from 10 to 60 seconds, with added validation and retry logic so onboarding completes successfully even when service removal is delayed.

3.0.4.2 Known Issues

The following sections provide a comprehensive list of known issues for the 3.0.4.2 release:

- **Table 4: System Management Known Issues**
- **Table 5: Network Management Known Issues**

Table 4: System Management Known Issues

Issue ID	Description
CNX - 235850	Installing HPE Aruba Networking Central On-Premises fails when using Kingston Data traveler Max (DTMAXA/512GB) USB Driver on HPE DL360 Gen10 servers. This issue occurs because the iLO server does not detect Kingston USB drive on the HPE DL360 Gen10 server.
CNX - 237437	In an **Air Gap** setup, the Web UI Interface is the recommended method for downloading and upgrading the new release build. It provides a more reliable option compared to the copadmin CLI menu.
CNX - 242947	After a firmware upgrade, the device configuration may go out of sync, causing a full configuration push. During this process, the device temporarily loses connectivity, which can cause the configuration push to fail and result in an automatic rollback. Once the device reconnects to HPE Aruba Networking Central On-Premises, the configuration is reimported. However, the Trust Anchor (TA) profile is not applied during this step beca=use reverse translation is not supported on Greenfield devices. **Workaround**: After the device reconnects to HPE Aruba Networking Central On-Premises, manually push the TA root certificate from HPE Aruba Networking Central On-Premises.
CNX - 245860	Adding a node after auto download fails because of an image synchronization failure on the new nodes. **Workaround**: Perform the **Add Node** operation before the auto download process or after the upgrade operation is complete.
CNX - 245881	In FIPS mode, USB - based ISO installation is not supported.

Table Continued

Issue ID	Description
CNX - 251591	During the HPE Aruba Networking Central On-Premises 3.0.30 installation, the following error message is displayed **CNX on - prem CREATE CLUSTER Stage - This stage creates a Kubernetes cluster of given nodes, has failed**. This issue occurs when the Virtual NIC is not reachable. **Workaround**: Perform the following steps on all nodes: **1.** Login to iLO server as an Administrator (for password contact the HPE Aruba Networking support team). **2.** Navigate to **Information** > **Diagnostics** > **Reset iLO**. **3.** Perform a factory reset on the node from which the setup cluster was initiated.
CNX - 253090	In the **Alert** context for a site, the **Defer** and **Clear** actions for active alerts remain stuck in the **In Progress** state and do not complete successfully.
CNX - 253899	When an upgrade is initiated on the disaster recovery (DR) cluster, the **Data - Sync** alert is not generated in the **System Alerts** page.
CNX-270110	Although Disaster Recovery (DR) operations complete successfully, the overall failover duration increases to approximately 2 hours. Increase in the time duration occurs because applications are restored and scaled up in batches during the failover process, extending the time required for all services to become fully operational after failover.
CNX-272192	During a system reboot, the reboot process gets stuck because running containers do not close before the reboot sequence is initiated. As a result, the reboot does not complete successfully, and SSH access remains unavailable. **Workaround**: If the reboot process becomes unresponsive, manually restart the server through the iLO server by performing a Power Off operation followed by a Power On operation.
CNX-277931	In HPE Aruba Networking Central On-Premises single-node deployments, backup operations are supported only for directory paths under `/home/<user>/`. Backup operations configured for other filesystem locations, such as `/tmp`, `/opt`, `/var`, `/build`, or their sub-directories (for example, `/tmp/test`, `/opt/test`, or `/var/test`), fail in single-node deployments. This does not affect multi-node clusters, where backup operations for these paths are supported.

Table Continued

Issue ID	Description
CNX-279955	As part of the ingress controller migration from the community nginx-onprem controller to the F5 NGINX Ingress Controller, the app-tier ingress ConfigMap was renamed from nginx-app-configuration to nginx-ingress-app. However, the certificate-settings backend (cop-platform-config) continues to reference only the legacy ConfigMap name. As a result, operations to enable or disable OCSP or modify strict certificate-check settings fails, and the updated values are not applied to the ingress configuration.
CNX-280049	In HPE Aruba Networking Central On-Premises 3.0.4.0, cluster upgrade fails intermittently during UPGRADE_INIT_APPS_INSTALL_ERROR stage. **Workaround**: **1.** Log in to the Cluster CLI, then execute the following commands sequentially:: **a.** crdn=$(kubectl get pods -n arango | grep crdn -m 1 | awk '{ print $1 }') **b.** kubectl exec -it -n arango $crdn -- arangosh --server.endpoint http+ssl://127.0.0.1:8529 --server.jwt-secret-keyfile /secrets/cluster/jwt/token **c.** db._useDatabase("gvtstatedb") **d.** db._collection("arango_failed_paths").truncate(); **e.** Exit the shell and the pod. **2.** Go to the browser and re-synchronize the init-arango-resource-manager application in ArgoCD.
CNX-280049	In HPE Aruba Networking Central On-Premises 3.0.4.0, cluster upgrade fails intermittently during application installation stage.
CNX-280085	Replace node operation fails when performed on the node where the setup wizard was originally run. **Workaround:** Contact the HPE Aruba Networking team.

Table Continued

Issue ID	Description
CNX-281228	On navigating to **Menu** > **System Management card** > **Configuration** > **Network tab**, the **Proxy** card display an incorrect error message **Failed to fetch proxy value**. This issue occurs in a newly installed HPE Aruba Networking Central On-Premises 3.0.4.0 setup when proxy settings have not yet been configured.
CNX-283200	In HPE Aruba Networking Central On-Premises single-node deployments, Restore operations fail during the ArangoDB restore stage because the ArangoDB pod became unhealthy. This issue is specific to single-node deployments and does not affect multi-node cluster deployments.

Table 5: Network Management Known Issues

Issue ID	Description
AOS-277233	Re-onboarding access points to using Zero Touch Provisioning (ZTP) fails for access points that were previously onboarded manually and upgraded to AOS 10.8.0.2. The issue occurs because during device detection when the AP attempts activate provisioning and a timing issue is triggered by prolonged blocking of DNS resolution. As a result, the AP is unable to log in to HPE Aruba Networking Central On-Premises. **Workaround:** Configure a DNS entry for device.arubanetworks.com and map it to a dummy IP address or the HPE Aruba Networking Central On-Premises VIP address. This allows the activate provisioning process to complete successfully and enables the AP to connect to HPE Aruba Networking Central On-Premises.
CNX-176290	The PATCH operation on the /network-config/v1alpha1/gateway-clusters/{name} API endpoint incorrectly allow modification requests for **Gateway Clustering Profiles** at child scopes (for example, group or site level). Gateway Clustering Profile updates at child scope must not be permitted.
CNX - 191954	AIOps is generating false VLAN Mismatch alerts for LAG and VSX interfaces, even when VLANs are configured and allowed on both switches."
CNX - 199108	Creating OSPF profiles over NBAPI with a **no - advertise - range** leaf specified throws an exception: **HPE_GL_ERROR_INTERNAL_SERVER_ERROR**.

Table Continued

Issue ID	Description
CNX - 210318	The Firmware Status column displays **Live upgrade scheduled** incorrectly for an AP even after the upgrade is completed and in certain cases even after the firmware policy is deleted. This issue occurs in the **Devices** table under **Firmware Management** page. It happens because an outdated status is sent after the upgrade and it remains in the database.
CNX - 228888	A Net Destination UI for IPv6 automatically deletes both colons (::) when trying to delete a single colon.
CNX - 230196	When a VLAN is used as an access VLAN on an interface, the system prevents its deletion and displays an error: **Validation Failure: VLAN '<ID>' cannot be deleted because it is referenced by Interface Ethernet '<Interface>' in the hierarchy**. However, if the VLAN is configured as a trunk VLAN with native VLAN as 1, the deletion succeeds silently, and the interface is configured to trunk all, with no warning or error messages. After deletion, the UI continues to display the deleted VLAN under the VLAN column, resulting in stale information.
CNX - 233454	The device enters a conflict state during Capability and Capacity (CNC) validation for DNS and NTP. This issue occurs because the UI fails to validate device capability limits, allowing configurations to be pushed beyond the supported limits.
CNX - 233604	Rogue devices on the Floorplan manager WebWebUI overlap due to having the same location. If a rogue device's location cannot be ascertained by location services, the location is assumed to be the same as the associated AP.
CNX - 235803	The number of sites displayed on the expanded **Sites** card does not match the count shown on the **Sites** tab under the **Configuration** menu.
CNX-235850	Installing HPE Aruba Networking Central On-Premises On-Premises fails when using Kingston Data traveler Max (DTMAXA/512GB) USB Driver on a HPE DL360 Gen10 servers. This issue occurs because the iLO server does not recognized the Kingston USB as HPE DL360 Gen10 is not incompatibility with Kingston USB.

Table Continued

Issue ID	Description
CNX-245266	VLAN profiles for gateways support three IP addresses, which can be configured as either static or dynamic. However, if **DHCP** is selected for one or more IP addresses, the WebUI does not allow static IP addresses to be configured for the other IP address fields. **Workaround:** Use APIs to configure the VLAN profile.
CNX - 245410	In the **Alerts** table, the displayed list of alerts may not match the actual alert count. Alerts generated successfully are intermittently missing from the Web UI, and are not consistently visible in either the **Active** or **Cleared** tabs.
CNX-250636	While configuring VSX, one of the VSX peers fails to receive the VSX configuration and goes out of sync. The configuration push fails with the following error: **"Device Fingerprint configuration should be removed before configuring link as Inter-Switch-Link".** **Workaround**: Disable the device fingerprinting and then create the VSX.
CNX-253386	User-based tunneling (UBT) clients are displayed as non-tunneled after opting out of GDPR. This is because client telemetry is event-based. **Workaround**: Disconnect and reconnect the client to trigger an event in the client telemetry pipeline.
CNX-253419	The **GDPR OPT-OUT** process fails to re-add clients to the UC list and trigger the GW Write Pipeline, leaving clients excluded from downstream processing.
CNX-254712	The creation of a VSF stack may fail because the VSF auto-stack configuration is not pushed to the switches. This issue affects HPE Aruba Networking Central On-Premises clusters that were initially deployed using releases prior to 3.0.2.0 and do not contain the required database schema updates.
CNX-261966	The device enters an out-of-sync state during Policy based routing, policy, or tunnel validation. This occurs when a previously deleted policy reappears as a stale entry and is pushed to the device. **Workaround:** Delete the policy, nexthop group, and tunnel using the DELETE API.

Table Continued

Issue ID	Description
CNX-263979	In HPE Aruba Networking Central On-Premises, the configuration status of the gateway is displayed as CONFIG_FAILIURE. This issue occurs when an invalid configuration is pushed, such as configuration of interface VLANs with DHCPv6 more than four VLANs at a given scope using Interface VLAN IPv6 Address Alias.
CNX-265528	The AP/Switch device context fails to retrieve content for the query and displays a **Failed to retrieve content** message. However, the same query returns valid results in the Global context.
CNX-268271	The VLAN interface create/update workflow fails to validate the **IPv6 Address/prefix** in the WebUI. As a result, invalid global **IPv6 addresses** are allowed instead of restricting input to valid global unicast **IPv6 addresses.**
CNX-268623	The connectivity path for UBT clients for AOS-CX switches may not be accurately displayed on the **Connectivity** card.
CNX-269017	Installing or Upgrade to HPE Aruba Networking Central On-Premises 3.0.3.4 could fail when the application installation or upgrade time exceeded the configured health timeout value. **Workaround**: Contact HPE Aruba Networking support team to verify that the application is healthy. After confirming the application's health status, retry the installation or upgrade operation.
CNX - 84012	In AP **System** profile, the **Static Channel** drop - down list for the Non - Preferred Scan Channels (PSC) **6 GHz** radio band fails to display dynamic options based on the selected county code.
CNX - 280078	On expanding the Insights card for the selected site, the **Access Point Firmware Recommendation** insight is not generated. This issue occurs because of a missing output data path.
CNX-280082	On expanding the Insights card for the selected site, the **Switch Firmware Recommendation** insight is not generated. This issue occurs because of a missing output data path.

API Change Log in 3.0.4.x Release

This topic lists the APIs updated in this release.

- **New MRT APIs**
- **New Configuration APIs**
- **Modified APIs**
- **Removed APIs**

New MRT APIs

Table 6: New MRT API List

Method	Path	Description
Monitoring > **IDPs**		
GET	/network-monitoring/v1/threats	This API is used to fetch the list of threats detected by the Suricata engine in the gateways.
GET	/network-monitoring/v1/threats/{id}	This API is used to fetch details information of a specific threat based on the threat ID.
Notification > **WIDS**		
GET	/network-services/v1/wids-intrusions	This API is used to fetch the list of wireless security events and intrusion alerts detected by the WIDS system. The API call supports filtering by site, event category (client/infrastructure), specific event types, severity levels, radio bands, and time ranges.
GET	/network-services/v1/wids-monitored-ap	This API is used to fetch wireless access points detected and monitored by the WIDS (Wireless Intrusion Detection System). The API call supports filtering by site, classification type, detection method, time ranges, containment status, and encryption protocols.
Services > **Location**		
GET	/network-services/v1/asset-tags/{asset-tag-id}/image	This API is used to fetch the asset tag image that was uploaded for the specified Asset id
PUT	/network-services/v1/asset-tags/{asset-tag-id}/image	This API is used to update the asset tag image for the specified Asset ID.

Table Continued

Method	Path	Description
DELETE	/network-services/v1/asset-tags/{asset-tag-id}/image	This API is used to delete an asset tag image for the specified Asset ID.
Notifications > **Notification Rules**		
GET	/network - notifications/v1/notification - rules	This API is used to fetch the list of notification rules. The notification rules list includes data source and destination channel details.
POST	/network - notifications/v1/notification - rules	This API is used to create a notification rule
GET, PATCH, or DELETE	/network - notifications/v1/notification - rules/{id}	These APIs are used to fetch, update, or delete the specified notification rule.
Reporting > **Reporting**		
POST	/network-reporting/v1/reports	This API is used to generate reports based on report-specific filters, report periods, and scheduling options. Reports can be scheduled for one-time or recurring execution and sent by email in multiple formats.
GET, PUT, or DELETE	/network-reporting/v1/reports/{report-id}	This API is used to fetch, update, or delete a specific user report by report ID. Report ID can be obtained from list reports API call (GET network-reporting/v1/reports) or in create Report API call (POST /network-reporting/v1/reports) response.
DELETE	/network-reporting/v1/reports/{report-id}/report-runs/{report-run-id}	This API deletes a specified report run using the report ID and report run ID. Report ID can be obtained from list reports API (GET network-reporting/v1/reports), and report run ID can be obtained using the list report Runs API (GET /network-reporting/v1/reports/{report-id}/report-runs).

Table Continued

Method	Path	Description
POST	/network-reporting/v1/reports/{report-id}/report-runs/{report-run-id}/download-link	This API is used to retrieve a downloadable link for a previously generated report run. Users can specify the export file format (CSV or PDF) by providing the appropriate exportType parameter in the request body. The response will contain the file's download URL, MIME type (application/zip for CSV file format and application/pdf for PDF file format), and the suggested file name for the report.
GET	/network-reporting/v1/reports-meta	This API is used to fetch reports metadata such as list of KPIS filters applicable for report types. This information is required when creating reports.
Services > **AirMatch**		
GET	/network-services/v1/airmatch-radio	This API is used to fetch radio reporting information for all radios in a tenant or for radios associated with a specific AP serial number when the AP Serial query parameter is provided.
GET	/network-services/v1/airmatch-radio/{radio-mac}	This API is used to fetch radio reporting information for a specific tenant based on the provided radio MAC address.
GET	/network-services/v1/airmatch-ap	This API is used to fetch access point (AP) information for all APs for a given tenant.
GET	network-services/v1/airmatch-ap/{serial-number}	This API is used to fetch access point (AP) information for a specified tenant based on the provided AP serial number.
GET	/network-services/v1/airmatch-ap-neighbor-list/{serial-number}	This API is used to fetch a list of neighboring Access Points (APs), identified by their serial numbers, for a specified AP within a given tenant.
GET	/network-services/v1/airmatch-priority-rf-events	This API is used to fetch all Priority Radio Frequency (RF) channel change events triggered by Radar detection or noise for a specified tenant.

Table Continued

Method	Path	Description
GET	/network-services/v1/airmatch-priority-rf-events/{radio-mac}	This API is used to fetch a list of Priority Radio Frequency (RF) events that triggered channel changes due to Radar detection or noise for a specified radio MAC address within a given tenant.
GET	/network-services/v1/airmatch-rf-events	This API is used to fetch all non-Priority Radio Frequency (RF) channel change events triggered by Radar detection or noise for a specified tenant.
GET	/network-services/v1/airmatch-rf-events/{radio-mac}	This API is used to fetch a list of non-Priority Radio Frequency (RF) events that triggered channel changes due to Radar detection or noise for a specified radio MAC address within a given tenant.
GET	/network-services/v1/airmatch-history/{radio-mac}	This API is used to fetch the radio history events for a specific Radio MAC address for a given tenant.
GET	/network-services/v1/airmatch-service-config	This API is used to fetch device running configuration for a given tenant.
GET	/network-services/v1/airmatch-global-config-id	This API is used to fetch the global configuration ID for the tenant.
GET	/network-services/v1/airmatch-radio-feasibility	This API is used to fetch the current radio feasibility for all radios for a given tenant.
GET	/network-services/v1/airmatch-radio-feasibility/{radio-mac}	This API is used to fetch the current radio feasibility for a specific radio MAC address for a given tenant.
GET	/network-services/v1/airmatch-board-limit/{serial-number}/{radio-mac}	This API is used to fetch the board limits of the radio for a given tenant.
GET	/network-services/v1/airmatch-device-config/{serial-number}	This API is used to fetch the device configuration for a specific AP Serial number for a given tenant.
GET	/network-services/v1/airmatch-non-friend/{radio-mac}	This API is used to fetch a list of non-friend (non-neighbor) radios for that radio MAC for a given tenant.
GET	/network-services/v1/airmatch-pathloss/{radio-mac}	This API is used to fetch all neighbors and pathloss information heard by a radio for a given tenant.

Table Continued

Method	Path	Description
GET	/network-services/v1/airmatch-partition	This API is used to fetch RF partition information for a specified tenant, including the list of radios in each partition, along with the associated RF domain and partition details.
POST	/network-services/v1/airmatch-partition	This API is used to send an RF Partition Request to Airmatch to create new RF partitioning based on current pathloss information.
GET	/network-services/v1/airmatch-radio-partition/{radio-mac}	This API is used to fetch the RF domain and friend partition id for a specific radio MAC address for a given tenant.
GET	/network-services/v1/airmatch-solution	This API is used to fetch the list of solver optimizations (solutions) generated by Airmatch for a specified tenant. It supports multiple query parameters for filtering and pagination. If no query parameters are provided, the API returns all available solutions for the tenant, subject to the default pagination limit.
POST	/network-services/v1/airmatch-runnow	This API is used to send an optimization request to Airmatch to compute and deploy a solution.
GET	/network-services/v1/airmatch-solution/{radio-mac}	This API is used to fetch solution or radio plan of a specific radio for a given tenant.
GET	/network-services/v1/airmatch-ap-coverage-plan	This API is used to fetch all AP coverage plan for a given tenant.
GET	/network-services/v1/airmatch-ap-coverage-plan/{serial-number}	This API is used to fetch the AP coverage plan for a given AP serial number for a tenant.
Service > **Audit Trail Information**		
GET	/network-services/v1/audits	This API is used to fetch all the audit logs based on the tenants.
GET	/network-services/v1/audits/{id}	This API is used to fetch the audit log entry for a given audit ID.
Monitoring > **Gateways**		
GET	/network-monitoring/v1/gateways/{serial-number}/modem-stat	This API is used to fetch the modem statistics data for the specified gateway.
Monitoring > **Application Visibility**		

Table Continued

Method	Path	Description
GET	/network-monitoring/v1/application-categories	This API is used to fetch the top N application categories ranked by total usage (TX + RX bytes) for the specified scope. The maximum supported time range is 7 days. If the interval between start-at and end-at exceeds 7 days, the start-at value is automatically adjusted to 7 days before end-at. This behavior is intentional, and no error is returned.
GET	/network-monitoring/v1/security-risks	The API is used to fetch a breakdown of application security risks (High, Medium, and Low) for the specified scope. The maximum supported time range is 7 days. If the interval between start-at and end-at exceeds 7 days, the start-at value is automatically adjusted to 7 days before end-at. This behavior is intentional, and no error is returned.
GET	/network-monitoring/v1/website-categories	This API is used to fetch the top N website categories ranked by total usage (TX + RX bytes) for the specified scope. The maximum supported time range is 7 days. If the interval between start-at and end-at exceeds 7 days, the start-at value is automatically adjusted to 7 days before end-at. This behavior is intentional, and no error is returned.

New Configuration APIs

Table 7: New Configuration APIs

Method	Path	Description
Security > **First Hop Security**		
GET	/network-config/v1alpha1/first-hop-security	This API is used to fetch the list of all configured First Hop Security profiles.
GET, POST, PATCH, or DELETE	/network-config/v1alpha1/first-hop-security/{name}	This API is used to fetch, create, update, or delete a specific First Hop Security profile.
Security > **DOS**		
GET	/network-config/v1alpha1/dos	This API is used to fetch the list of all configured DoS (Denial of Service) profiles.
GET, POST, PATCH, or DELETE	/network-config/v1alpha1/dos/{name}	This API is used to fetch, create, update, or delete a specific DoS profile.

Table Continued

Method	Path	Description
System > **Hardware Module Device**		
GET	/network-config/v1alpha1/hardware-module	This API is used to fetch the list of hardware module profiles. A hardware module profile defines device-specific hardware configuration for a standalone switch, a chassis line module, or a VSF stack member. Each profile targets a specific device type and encapsulates the hardware settings applicable to that type, enabling consistent configuration across devices of the same kind.
GET, POST, PATCH, or DELETE	/network-config/v1alpha1/hardware-module/{name}	These APIs are used to fetch, create, update, or delete a specific hardware module profile.

Modified APIs

- **Table 8: Modified MRT APIs**
- **Table 9: Modified Configuration APIs**

Table 8: Modified MRT APIs

Method	Description
Monitoring > **Access Points**	
GET /network-monitoring/v1/aps	The API response is enhanced to include the **gatewayClusters** parameter. When an AP has one or more connected tunnels that are part of a gateway cluster, the associated gateway cluster name is returned in this parameter.
GET /network-monitoring/v1/wlans	The API response is enhanced to include **client_count** for the WLAN list.
Monitoring > **Site Health**	
GET /network - monitoring/v1/site - health/{site - id}	This API only support the **site - id** parameter. To get the **site - id** use **the GET /network - monitoring/v1/sites - health** using the **siteName** filter.
Monitoring > **Access Point**	
GET /network-monitoring/v1/aps/{serial-number}	The API response now includes the **is_uplink** parameter to identify whether a port is currently configured and operating as an uplink.

Table Continued

Method	Description
GET/network-monitoring/v1/wlans/{wlan-name}	The API response is enhanced to include the **client_count** for the specified WLAN.
Notifications > **Alerts**	
GET /network-notifications/v1/alerts/clear	This API is updated to make the reason field a mandatory parameter in the request body.
Troubleshooting > **Events**	
GET /network-troubleshooting/v1/events	The sort field in this API is updated to use **timeAt** instead of **timestamp**.
Troubleshooting > **AOS-CXSwitches** **Troubleshooting** > **CX Switches**	
For switch stacks, the APIs listed under AOS-CX Switches and CX switches support the use of either the conductor serial number or the stack ID in the **serial-number** path parameter.	

Table 9: Modified Configuration APIs

Method	Description
Named Object > **Alias**	
POST /network - config/v1alpha1/aliases/{name}	This API is updated to allow **ALIAS_IPV6_SYSTEM_VLAN** to be selected as the value of the **type** parameter.
System > **Gw System**	
POST /network - config/v1alpha1/gw - system/{name}	This API is updated to allow **ipv6 - device - vlan - alias** to be configured.
System > **Switch System**	
The **Switch System** APIs are enhanced to configure the client insight parameters. The following parameters are added to the Switch System APIs: • enable— Enable or disable the Client Insight feature, which captures L2, L3, and L4 onboarding details of clients connected to the switch. The details are published to HPE Aruba Networking Central On-Premises and provides enhanced visibility into client activities. Available on AOS-CX and ArubaOS switches. • onboarding-event-log— Enable or disable client onboarding status event logging. When enabled, the switch generates event logs for each client's onboarding outcome (success/failure with reason codes). Requires Client Insight to be enabled. Available on AOS-CX switches only.	
Security > **Firewall**	

Table Continued

Method	Description
The APIs listed under the Firewall is updated with the following changes: **IPv4 Container** • The **attack-rate** parameter is removed from the IPv4 container. This parameter can now be configured using the DoS API. • The **cp-bandwidth-contract** parameter is removed from the **IPv4** container. This parameter can now be configured using the **Control Plane Policies** API. • The **local-valid-users**, **prevent-dhcp-exhaustion, prohibit-arp-spoofing**, **prohibit-ip-spoof-all**, and **prohibit-ip-spoofing** parameters are removed from the **IPv4** container. These parameters can now be configured using the First Hop Security API. **IPv6 Container** • The **attack-rate** parameter is removed from the IPv6 container. This parameter can now be configured using the DoS API. • The **enable-stateful-icmp**, **enforce-tcp-handshake**, and **enforce-tcp-sequence** parameters are removed from the **IPv6** container. These parameters can now be configured using the **GW System** API.	
Configuration Health > **Configuration Health**	
GET /network-config/v1alpha1/config-health/active-issue	This API is enhanced to include **additionalInfo** parameter in the response body. Additional information about the distribution failure is displayed.
GET /network-config/v1alpha1/config-health/devices	This API is enhanced to include **serialNumber** parameter in the response body.
Interfaces > **Interface Loopback**	
POST /network-config/v1alpha1/loopback-interfaces/{id}	The following parameters are listed as deprecated: • ipv4 • ipv4-prefix • ipv6-address • ipv6-addresses • link-local • secondary-ip The above parameters can be configured using the **ipv4-config** and **ipv6-config** containers.

Removed APIs

Table 10: Removed API List

Removed APIs	Alternate APIs
All alpha **MRT APIs** (**v1alpha1**, and **v1alpha2**) are removed. You must use the corresponding **v1** APIs.	